Department of Information Technology

Cybersecurity Best Practices & Data Loss Prevention (DLP)

Maria S. Thompson
State Chief Risk Officer

Cybersecurity Best Practices

- Increasing Cybersecurity breaches and shrinking budgets result in heavier focus to maximize cyber investments
- Traditional methods involved the purchase of new capabilities to mitigate and reduce the attack surface.
- Current and future efforts will be a balance between leveraging present capabilities and staying abreast with the changing cyber landscape. These efforts include, but are not limited to:
  - Cyber Hygiene
  - Speed to Threat Detection & Response
  - First Line of Defense
  - Information Sharing
  - Assurance from Third Party providers

Cyber Hygiene

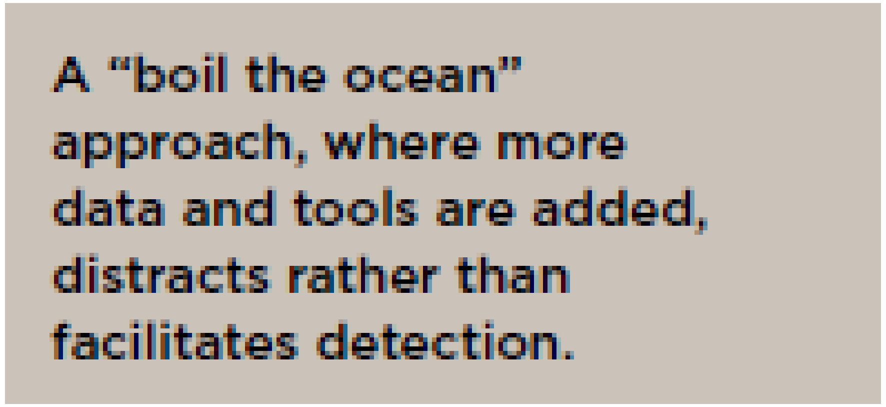
- Top down support for cyber hygiene must be present. Understand that operational convenience can lead to data breaches.
- Adopt an industry best practice security framework:
  - Define standard core security controls across the enterprise
  - Accountability
- Develop a Continuous Monitoring Plan to assess the state of the security controls.
- Implement a robust patch management program.
- Data Management
- Prioritization of risks
- Utilization of metrics and measurement

99.9% of successful exploits in 2014 was as a result of a vulnerability that was more than **1 year old**.

Source: CEB Analysis, Verizon Data Breach Report, Mandiant Report

Threat Detection & Response

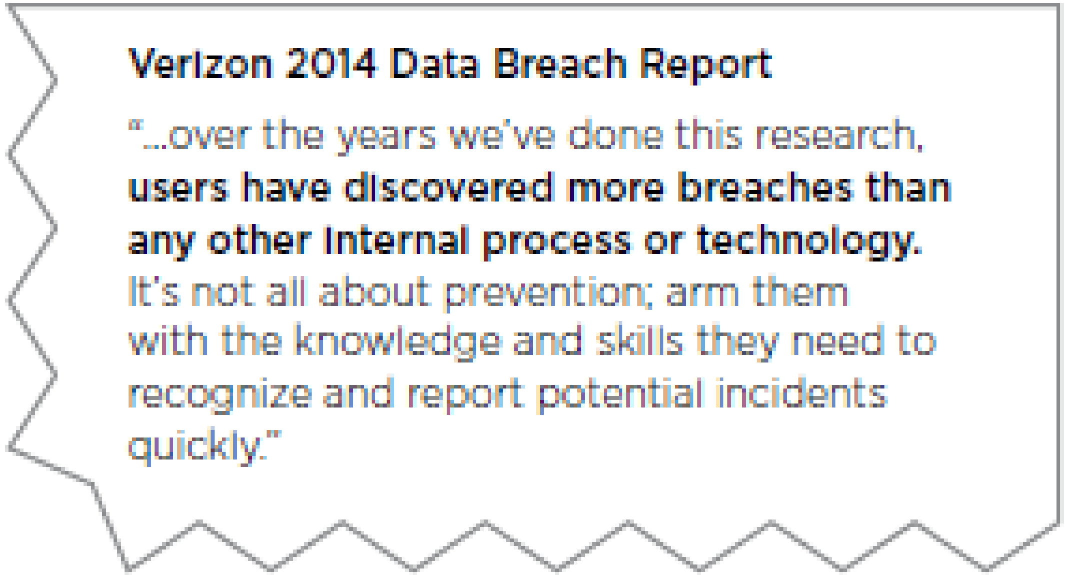
- Increase the ability for timely detection of anomalous behavior
  - Research shows on average, it takes respondents 256 days to identify a breach caused by a malicious attacker, and 82 days for containment.
  - There is a direct correlation between time to detect and overall cost of a breach.



A "boil the ocean" approach, where more data and tools are added, distracts rather than facilitates detection.

First Line of Defense

- Invest in the employee cyber awareness training.
- Employees become early warning system for reporting incidents.
- Ensure employees are aware of what is acceptable use of IT.
- Measure employees responses to security incidents.



Verizon 2014 Data Breach Report

"...over the years we've done this research, **users have discovered more breaches than any other internal process or technology.** It's not all about prevention; arm them with the knowledge and skills they need to recognize and report potential incidents quickly."

Assurance from 3rd Party Providers

- **TRANSPARENCY**: Ability to assess third party vendors on a pre-determined basis.
- Define a standard, repeatable assessment model for vendors to use.
- Ensure contracts clearly articulate vendor requirements, frequency and repercussions for failure to meet compliance standards.
- Some states require third party cloud vendors to have cyber insurance.

Source: CEB Analysis, Verizon Data Breach Report, Mandiant Report

Data Loss Prevention (DLP)

DIT’s Strategic Goals for Data Loss Prevention (DLP)

- Reduce the risks associated with the unintentional and intentional disclosure of sensitive data in use and in transit.
  - Future plans involve DLP Data at Rest compliance.
  - Ensure that authorized transmission of sensitive data to 3rd parties, occur via approved methods.
- Protect citizen’s data and maintain the state’s reputation.
- Aid in compliance with federal, state and other regulatory requirements.
- Provide functionalities to support the business unit while maintaining adequate security.
- Accountability for data management

Questions?